(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平10－107787

(43)公開日　平成10年(1998)4月24日

(51)Int.Cl.*		識別記号	FI		
H04L	9/08		H04L	9/00	601B
G06F	12/14	320	G06F	12/14	320B
	15/00	330		15/00	330Z
G09C	1/00	660	G09C	1/00	660B
H04L	9/14		H04L	9/00	641

審査請求　未請求　請求項の数70　ＦＤ　(全 22 頁)　最終頁に続く

(21)出願番号　特願平8－277125

(22)出願日　平成8年(1996)9月27日

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内2丁目6番3号

(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目6番3号　三菱商事株式会社内

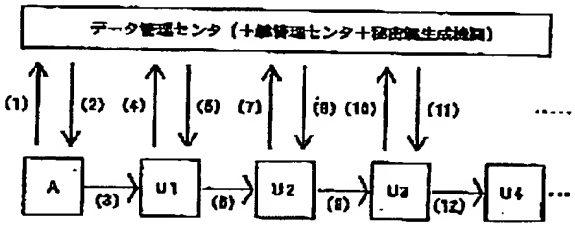
(74)代理人　弁理士　雨笠　貞一郎

(54)【発明の名称】　データ管理システム

(57)【要約】　(修正有)

【課題】　ネットワークでのデータの安全を確保する。

【解決手段】　(1)原著作者Aは原著作権ラベルL。を提示して原秘密鍵K。。の配布をデータ管理センタC。に要求。(2)センタC。は、ラベルL。と共に、対応させた原秘密鍵K。。をAの公開鍵K。。で暗号化し、暗号化原秘密鍵C。。O。。をAに配布。このときセンタC。はラベルL。を一方向ハッシュし、ラベル指紋F。を作成しAに配布。(3)Aは暗号化原秘密鍵C。。O。。をAの専用鍵で復号し、復号された原秘密鍵K。。で原著作物データM。を暗号化し、暗号化原著作物データとラベルL。及びラベル指紋F。を最初のユーザU₁に転送。(4)U₁は、ラベルL。とラベル指紋F。及び第1ユーザラベルL。₁とC。に提示して、原及び第1秘密鍵K。₁の配布を求める。(5)C。はL。の正当性をラベル指紋F。で確認し、L₁の登録と共に、K。。。K。₁をU₁の公開鍵で暗号化しU₁へ配布。(6)U₁はU₁の専用鍵で復号し、このK。。で暗号化データを復号する。



【特許請求の範囲】

【請求項１】通信ネットワークを介してデータ所有者からデータ利用者に転送されるデジタルデータを管理するデータ管理システムであって：前記データ管理システムでは、秘密鍵，公開鍵，専用鍵，データ所有者ラベル，データ利用者ラベル及びデータラベルが使用され；データ管理センタが公開鍵保管機関及び秘密鍵生成機関とリンクして前記通信ネットワーク上に配置され；前記データ管理センタは前記データ所有者及び前記データ利用者の公開鍵の認証を行うとともに前記データ所有者ラベル，前記データ利用者ラベル及び前記データラベルを保管しており；前記データ所有者がデータ所有者ラベル及びデータラベルを提示して前記データ管理センタにデータ暗号化用の秘密鍵を要求し；前記データ管理センタは前記データラベルからデータラベル指紋を作成し、前記データラベル指紋及び前記データ所有者の公開鍵を用いて暗号化された暗号化用秘密鍵を前記データ所有者に配付し；前記データ所有者は前記データ所有者の専用鍵を用いて復号された前記秘密鍵を用いてデータを暗号化し、前記暗号化データ，前記データラベル及び前記データラベル指紋を最初のユーザに転送し；前記最初のデータ利用者が前記最初のデータ利用者のユーザラベル，前記データラベル及び前記データラベル指紋を提示して、前記データ管理センタに前記暗号化データを復号するための秘密鍵と復号された前記データ再暗号化するための秘密鍵を要求し；前記データ管理センタが前記データラベル指紋により前記データラベルの正当性を確認し、前記最初のデータ利用者のユーザラベルを登録するとともに、前記暗号化データを復号するための秘密鍵と復号された前記データ再暗号化するための秘密鍵を前記最初のデータ利用者の公開鍵を用いて暗号化して前記最初のデータ利用者に配布し：前記最初のデータ利用者は、前記最初のデータ利用者の専用鍵を用いて前記復号化用秘密鍵と前記再暗号化用秘密鍵を復号し、前記復号化用秘密鍵を用いて暗号化データを復号して利用し、復号された前記データを前記再暗号化用秘密鍵を用いて暗号化して保存，複写し、前記暗号化データをデータラベル，データラベル指紋及び最初のデータ利用者のユーザラベルとともに次のデータ利用者に転送する。

【請求項２】　前記データ所有者が前記データ所有者ラベル及び前記データラベルをデータ管理センタに提示することにより、著作権登録が行われる請求項１記載のデータ管理システム。

【請求項３】　データの利用者により前記データの加工が行われ、前記データの加工内容が前記データラベルに付加される、請求項１記載のデータ管理システム。

【請求項４】　前記データ利用者が前記データの利用者ラベル及び前記加工内容が記載されたデータラベルをデータ管理センタに提示することにより、二次著作権登録が行われる請求項３記載のデータ管理システム。

【請求項５】　前記データが複数である、請求項３又は請求項４のデジタルデータ管理システム。

【請求項６】　前記データラベルにデジタル署名が行われる、請求項１，請求項２，請求項３，請求項４又は請求項５記載のデータ管理システム。

【請求項７】　前記データ利用者が前記利用者ラベル及び前記データラベルをデータ管理センタに提示したことに基づいて課金が行われる請求項１，請求項２，請求項３，請求項４，請求項５又は請求項６記載のデータ管理システム。

【請求項８】　前記課金が使用実績メータリング後払い方式によって行われる請求項７記載のデータ管理システム。

【請求項９】　前記使用実績メータリングデータがデータ管理センタに保管される請求項８記載のデータ管理システム。

【請求項１０】　前記使用実績メータリングデータが利用者の装置に保管される請求項８記載のデータ管理システム。

【請求項１１】　前記課金が前払い方式によって行われる請求項７記載のデータ管理システム。

【請求項１２】　前記前払いのデータがデータ管理センタに保管される請求項１１記載のデータ管理システム。

【請求項１３】　前記前払いのデータが利用者の装置に保管される請求項１１記載のデータ管理システム。

【請求項１４】　前記デジタルデータが通常のファイル構造を有しており、データボディのみが暗号化されている請求項１，請求項２，請求項３，請求項４，請求項５，請求項６，請求項７，請求項８，請求項９，請求項１０，請求項１１，請求項１２又は請求項１３記載のデータ管理システム。

【請求項１５】　前記データボディの一部が暗号化されている請求項１４記載のデータ管理システム。

【請求項１６】　前記データボディの一部が連続的に暗号化されている請求項１５記載のデータ管理システム。

【請求項１７】　前記データボディの一部が不連続に暗号化されている請求項１５記載のデータ管理システム。

【請求項１８】　前記デジタルデータが通常のファイル構造を有しており、データヘッダとデータボディが暗号化されている請求項１，請求項２，請求項３，請求項４，請求項５，請求項６，請求項７，請求項８，請求項９，請求項１０，請求項１１，請求項１２又は請求項１３記載のデータ管理システム。

【請求項１９】　前記データヘッダの一部と前記データボディの全部が暗号化されている請求項１８記載のデータ管理システム。

【請求項２０】　前記データヘッダの一部とデータボディの一部が暗号化されている請求項１８記載のデータ管理システム。

【請求項２１】　前記デジタルデータが通常のファイル

構造を有しており、データヘッダのみが暗号化されている請求項1．請求項2．請求項3．請求項4．請求項5．請求項6．請求項7．請求項8．請求項9．請求項10．請求項11．請求項12又は請求項13記載のデータ管理システム。

【請求項22】　前記データヘッダの全部が暗号化されている請求項21記載のデータ管理システム。

【請求項23】　前記データヘッダの一部のみが暗号化されている請求項21記載のデータ管理システム。

【請求項24】　前記デジタルデータが通常のファイル構造を有しており、著作権ラベルのみが暗号化されている請求項1．請求項2．請求項3．請求項4．請求項5．請求項6．請求項7．請求項8．請求項9．請求項10．請求項11．請求項12又は請求項13記載のデータ管理システム。

【請求項25】　前記著作権ラベルの一部のみが暗号化されている請求項24記載のデータ管理システム。

【請求項26】　前記デジタルデータがオブジェクト形式のファイル構造を有しており、メソッドが暗号化されている請求項1．請求項2．請求項3．請求項4．請求項5．請求項6．請求項7．請求項8．請求項9．請求項10．請求項11．請求項12又は請求項13記載のデータ管理システム。

【請求項27】　放送，通信ネットワークあるいはデータ蓄積媒体を介してデータ所有者からデータ利用者に転送されるデジタルデータを管理するシステムであって：該データ管理システムでは、公開鍵，専用鍵，データ利用者ラベル及びデータラベルが使用され；データ管理センタ及びデータ所有者が公開鍵保管機関とリンクして前記通信ネットワーク上に配置され；前記データ管理センタが前記データ所有者及び前記データ利用者の公開鍵の認証を行うとともに前記データ利用者ラベル及び前記データラベルを保管しており；最初のデータ利用者がデータ利用者ラベルを提示して前記ネットワーク内からデータ及びデータラベルを入手して利用し、利用終了後は前記データが前記データ利用者の装置内に保存されない。

【請求項28】　前記データが消去されることにより、前記データ利用者の装置内に保存されない請求項27記載のデータ管理システム。

【請求項29】　前記データが一方向ハッシュ値化されることにより、前記データ利用者の装置内に保存されない請求項27記載のデータ管理システム。

【請求項30】　前記データ管理センタが秘密鍵生成機関とさらにリンクしており、前記データが秘密鍵を用いて暗号化されて、前記データ利用者の装置内に保存される請求項27記載のデータ管理システム。

【請求項31】　データの加工が行われ、データの加工内容が前記データラベルに付加されることにより加工ラベルが得られる、請求項28．請求項29又は請求項30記載のデータ管理システム。

【請求項32】　前記加工ラベルのみが次のデータ利用者に転送される請求項31記載のデータ管理システム。

【請求項33】前記加工ラベルが前記次のユーザの公開鍵を用いて暗号化されて前記次のデータ利用者に転送され；前記次のデータ利用者が前記暗号化加工ラベルを前記次のデータ利用者の専用鍵を用いて復号し、復号された前記加工ラベルを前記データ管理センタに提示し；前記データ管理センタが前記加工ラベルに基づきデータを前記次のデータ利用者に転送し；前記次のユーザが前記加工ラベルの加工データによりデータを加工して利用する、請求項32記載のデータ管理システム。

【請求項34】　前記最初の利用者が前記加工データを前記次のユーザに転送し；前記次のデータ利用者が前記次のデータ利用者が前記加工データを前記データ管理センタに提示し；前記データ管理センタが前記加工ラベルに基づきデータを前記次のデータ利用者に転送し；前記次のユーザが前記加工ラベルの加工データによりデータを加工して利用する、請求項32のデータ管理システム。

【請求項35】　前記最初の利用者が前記最初の利用者の専用鍵を用いて前記加工ラベルにデジタル署名を行う、請求項34記載のデータ管理システム。

【請求項36】　データが複数である、請求項28．請求項29．請求項30．請求項31．請求項32．請求項33．請求項34又は請求項35記載のデジタルデータ管理システム。

【請求項37】　前記データ利用者が前記利用者ラベル及び前記データラベルをデータ管理センタに提示したことに基づいて課金が行われる請求項27．請求項28．請求項29．請求項30．請求項31．請求項32．請求項33．請求項34．請求項35又は請求項36記載のデータ管理システム。

【請求項38】　前記課金が使用実績メータリング後払い方式によって行われる請求項37記載のデータ管理システム。

【請求項39】　前記使用実績メータリングデータがデータ管理センタに保管される請求項38記載のデータ管理システム。

【請求項40】　前記使用実績メータリングデータが利用者の装置に保管される請求項38記載のデータ管理システム。

【請求項41】　前記課金が前払い方式によって行われる請求項37記載のデータ管理システム。

【請求項42】　前記前払いのデータがデータ管理センタに保管される請求項41記載のデータ管理システム。

【請求項43】　前記前払いのデータが利用者の装置に保管される請求項41記載のデータ管理システム。

【請求項44】　前記デジタルデータが通常のファイル構造を有しており、データボディのみが暗号化されている請求項28．請求項29．請求項30．請求項31．

請求項32，請求項33，請求項34，請求項35，請求項36，請求項37，請求項38，請求項39，請求項40，請求項41，請求項42又は請求項43記載のデータ管理システム。

【請求項45】　前記データボディの一部が暗号化されている請求項44記載のデータ管理システム。

【請求項46】　前記データボディの一部が連続的に暗号化されている請求項45記載のデータ管理システム。

【請求項47】　前記データボディの一部が不連続に暗号化されている請求項45記載のデータ管理システム。

【請求項48】　前記デジタルデータが通常のファイル構造を有しており、データヘッダとデータボディが暗号化されている請求項28請求項29，請求項30，請求項31，請求項32，請求項33，請求項34，請求項35，請求項36，請求項37，請求項38，請求項39，請求項40，請求項41，請求項42又は請求項43記載のデータ管理システム。

【請求項49】　前記データヘッダの一部と前記データボディの全部が暗号化されている請求項48記載のデータ管理システム。

【請求項50】　前記データヘッダの一部とデータボディの一部が暗号化されている請求項48記載のデータ管理システム。

【請求項51】　前記デジタルデータが通常のファイル構造を有しており、データヘッダのみが暗号化されている請求項28請求項29，請求項30，請求項31，請求項32，請求項33，請求項34，請求項35，請求項36，請求項37，請求項38，請求項39，請求項40，請求項41，請求項42又は請求項43記載のデータ管理システム。

【請求項52】　前記データヘッダの全部が暗号化されている請求項51記載のデータ管理システム。

【請求項53】　前記データヘッダの一部のみが暗号化されている請求項51記載のデータ管理システム。

【請求項54】　前記デジタルデータが通常のファイル構造を有しており、著作権ラベルのみが暗号化されている請求項27，請求項28請求項29，請求項30，請求項31，請求項32，請求項33，請求項34，請求項35，請求項36，請求項37，請求項38，請求項39，請求項40，請求項41，請求項42又は請求項43記載のデータ管理システム。

【請求項55】　前記著作権ラベルの一部のみが暗号化されている請求項54記載のデータ管理システム。

【請求項56】　前記デジタルデータがオブジェクト形式のファイル構造を有しており、メソッドが暗号化されている請求項27，請求項28請求項29，請求項30，請求項31，請求項32，請求項33，請求項34，請求項35，請求項36，請求項37，請求項38，請求項39，請求項40，請求項41又は請求項42又は請求項43記載のデータ管理システム。

【請求項57】　需要者と生産者との間で仲介業者を介して行われる商取引システムであって：該商取引システムでは、秘密鍵，公開鍵－専用鍵が使用され；前記仲介業者が公開鍵保管機関及び秘密鍵生成機関とリンクして通信ネットワーク上に配置され；前記需要者が前記仲介業者に商取引データを要求し；前記仲介業者は前記生産者の公開鍵を用いて暗号化された暗号化用秘密鍵とともに前記需要者の商取引データ要求を前記生産者に転送し；前記生産者は前記生産者の専用鍵を用いて前記暗号化用秘密鍵を復号し、前記復号された暗号化用秘密鍵を用いて前記商取引データを暗号化して前記仲介業者に送付し；前記仲介業者は前記暗号化用秘密鍵を用いて前記暗号化商取引データを復号し、復号された前記商取引データを再暗号化用秘密鍵を用いて再暗号化して前記需要者の公開鍵を用いて暗号化された前記再暗号化用秘密鍵とともに前記需要者に転送し；前記需要者は前記需要者の専用鍵を用いて前記再暗号化用秘密鍵を復号し、前記復号された再暗号化用秘密鍵を用いて前記暗号化商取引データを復号し、前記復号された商取引データに発注事項を記入して発注書を作成し、前記発注書を前記再暗号化用秘密鍵を用いて暗号化し、前記再暗号化発注書を前記仲介業者に送付し；前記仲介業者は前記再暗号化用秘密鍵を用いて前記再暗号化発注書を復号し、前記復号された発注書を前記生産者の公開鍵を用いて暗号化し、前記暗号化発注書を前記生産者に転送し；前記生産者は前記生産者の専用鍵を用いて前記暗号化発注書を復号し、受注処理を行う。

【請求項58】　前記デジタルデータが通常のファイル構造を有しており、データボディのみが暗号化されている請求項57記載のデータ管理システム。

【請求項59】　前記データボディの一部が暗号化されている請求項58記載のデータ管理システム。

【請求項60】　前記データボディの一部が連続的に暗号化されている請求項59記載のデータ管理システム。

【請求項61】　前記データボディの一部が不連続に暗号化されている請求項59記載のデータ管理システム。

【請求項62】　前記デジタルデータが通常のファイル構造を有しており、データヘッダとデータボディが暗号化されている請求項57記載のデータ管理システム。

【請求項63】　前記データヘッダの一部と前記データボディの全部が暗号化されている請求項62記載のデータ管理システム。

【請求項64】　前記データヘッダの一部とデータボディの一部が暗号化されている請求項62記載のデータ管理システム。

【請求項65】　前記デジタルデータが通常のファイル構造を有しており、データヘッダのみが暗号化されている請求項57記載のデータ管理システム。

【請求項66】　前記データヘッダの全部が暗号化されている請求項65記載のデータ管理システム。

【請求項67】　前記データヘッダの一部のみが暗号化されている請求項65記載のデータ管理システム。
【請求項68】　前記デジタルデータが通常のファイル構造を有しており、著作権ラベルのみが暗号化されている請求項57記載のデータ管理システム。
【請求項69】　前記著作権ラベルの一部のみが暗号化されている請求項68記載のデータ管理システム。
【請求項70】　前記デジタルデータがオブジェクト形式のファイル構造を有しており、メソッドが暗号化されている請求項57記載のデータ管理システム。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、デジタルデータの管理、特に著作物データの著作権管理、電子商取引、電子通貨に有効に適用されるデジタルデータ管理システムに係るものである。
【0002】
【従来の技術】情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム2値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。
【0003】各種電気信号のディジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた2値データ以外の画像信号もディジタル処理技術の開発が進められている。この画像信号のディジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をディジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。
【0004】画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままでは保存，転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用のＪＰＥＧ（Joint Photographic image coding ExpertsGroup）規格，テレビジョン会議用のH.261規格，画像蓄積用のＭＰＥＧ１（Moving Picture image coding Experts Group 1）規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するＭＰＥＧ２規格が作成された。これらの技術により、ディジタル映像データのリアルタイム処理が可能となってきている。
【0005】従来広く普及しているアナログデータは保存，複写，加工，転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、ディジタルデータは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、ディジタルデータの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもディジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。
【0006】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存，複写，加工することによって有効活用し、加工したデータを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータである音声データ及び画像データがディジタル化されてデータベースとされる。
【0007】このような状況において，データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段，特に，複写，加工，転送等の2次利用について完成された著作権管理手段はない。
【0008】一方、これまでは比較的小さな規模で行われていたコンピュータを用いたデータ通信で、ここ数年インターネットと呼ばれるコンピュータ通信システムが急速に普及し、あらゆる人々にとって身近な存在となりつつある。このインターネットシステムで通信される情報は当初は文字情報のみであったが、技術の進展にしたがって、音声データ及び画像データが取り扱われ、さらには信頼性及び秘密性が重要である電子商取引データあるいは電子通貨データまでがインターネットシステムで取り扱われようとしている。
【0009】このような中で、取り扱われるデータの秘密性，信頼性に関する安全性の保証技術、課金が必要な場合の課金技術の確立の必要性が要望されている。
【0010】利用に対して課金される著作物データについては著作権の主張がなされていることが多いが，著作物データの中には個人メール，広告・宣伝等著作権を積極的に主張しないものがある。例えば，著作権の主張を伴わない個人メールの場合にはプライバシーの確保，内容改竄防止及び偽造防止が重要である。また，通常は著作権の主張を行わない広告・宣伝用のデータであっても、内容の改竄による被害の発生、非対象者への配布あるいは偽データによる営業の混乱が発生することがあ

る。このように、個人メールにあっては内容の改竄防止、プライバシー侵害防止及び偽造防止が必要であり、広告・宣伝データにあっては内容の改竄防止、閲覧制限及び偽造防止が必要である。

【0011】個人メールのプライバシー侵害防止及び広告宣伝データの閲覧制限はデータの暗号化によって実現することができ、個人メール及び広告宣伝データの偽造防止、個人メール及び広告・宣伝データの改竄防止は発信者の確認（認証）により実現される。

【0012】草の根的な発想を有するインターネットシステムはシステム自体のセキュリティは非常に脆弱である。インターネットシステムのセキュリティを確保するためのシステムが提案され、代表的なシステムとして階層構造を採るＰＥＭ（Privacy Enhanced Mail）と水平分散構造を採るＰＧＰ（Pretty Good Privacy）がある。これらはいずれもデータの親展性、発信元の認証、データの無改竄証明、最初の発信者の表示及び公開鍵の管理を行うが、データの加工を含む再利用の制限は何れも不可能である。

【0013】階層構造を採るＰＥＭでは、ＩＰＲＡ(Internet PCA Registration Authority)と呼ばれる最上位の機関と、ＰＣＡ(Policy Certification Authority)と呼ばれる次位の機関と組織(Organizational)、地域（Residential)、個人(Personal)と各々呼ばれる最下位の機関から構成され、上位の保証機関(Certifucation Authorityies)が下位の機関の公開鍵について下位の機関の氏名等のデータにデジタル署名した公開鍵証明書を発行することによりその公開鍵の正当性を保証する。

【0014】水平分散構造を採るＰＧＰでは、ＰＥＭのCertifucation Authorityに相当する機関はなく、信用できる他人が公開鍵の氏名等のデータにデジタル署名した公開鍵証明書を発行することによりその公開鍵の正当性を保証する。このＰＧＰには公開鍵の簡易確認方法として公開鍵をＭＤ５(Message Digest 5)等の一方向ハッシュ(hash)関数によってハッシュした１６バイトのハッシュ値を音声によって確認する電子指紋と呼ぶ方法がある。

【0015】ＰＥＭとＰＧＰを比較した場合、階層構造を採るＰＥＭでは認証者についての問題はないが、草の根的なインターネットシステムでは必ずしも一般的なシステムであるとはいえない。一方、ＰＧＰは簡便であり一般的に広く採用可能なシステムではあるが、信頼できる署名者が見あたらない場合には利用することができない。

【0016】ところで、コンピュータネットワークシステムの発展に伴い従来はスタンドアローンで使用されていた個々のコンピュータがネットワークシステムを介して接続され、データを共有するデータベースシステムが普及し、データだけでなくアプリケーションプログラム、さらにはオペレーティングシステムと呼ばれる基本ソフトウェアまでもネットワークを介して共有する分散オブジェクトシステムも提案されている。

【0017】分散オブジェクトシステムは、データもソフトウェアもともにプログラムとデータからなるオブジェクトとして、サーバから供給される。分散オブジェクトシステムには、オペレーティングシステム、アプリケーションプログラム及びデータはサーバが提供し、データ処理及びデータ保存は通常のコンピュータであるユーザ端末装置で行うオブジェクトコンテナと呼ばれるシステムと、オペレーティングシステム、アプリケーションプログラム及びデータはサーバが提供し、データ処理はネットワークコンピュータと呼ばれるユーザ端末装置が行うがデータの保存はサーバが行うサーバオブジェクトサーバと呼ばれるシステムがある。このサーバオブジェクトサーバシステムはさらに押し進めて、データ処理もサーバが行い、ユーザ端末装置は入出力の機能のみしか有せず、システム全体が一つのコンピュータとして機能するものまでが考えられている。

【0018】また、ネットワークシステムの別の形態として、通信回線等のネットワーク基盤を提供する事業者が通信回線以外の課金システム、セキュリティシステム、著作権管理システム、認証システム等を提供し、サービス事業者がこれらのシステムサービスを利用してあたかも自己のシステムのようにしてネットワーク事業を行うライセンスネットワークと呼ばれる「貸貸ネットワークシステム」も構想されている。

【0019】

【発明の概要】発明者は本出願において、通常のコンピュータネットワークシステム、分散オブジェクトシステム及びライセンスネットワークシステムにおけるデジタルデータ著作権保護、電子商取引データの安全性確保、電子通貨データの安全性確保を実現するためのデジタルデータ管理システムを提案する。

【0020】第１のデジタルデータ管理システムはネットワーク上のデータ管理センタとネットワークを利用する原著作権者あるいは情報提供者と複数のユーザから構成されている。データ管理センタはネットワーク利用者の公開鍵の認証とユーザラベル提示に対するデータ暗号化秘密鍵の配布を行うとともに秘密鍵の要求によるデータ利用状況の把握を行う。データは秘密鍵を用いて暗号化されて保存・転送されるが、保存・転送するデータは転送されたデータの秘密鍵とは異なる秘密鍵で暗号化される。また、原データには原データラベルが、加工データには加工データラベルが付加され、データ管理センタはデータの保管は行わず原データラベル及び加工データの保管のみを行う。秘密鍵の要求にユーザラベルが使用されるが、代わりにユーザラベルの電子指紋を使用することもできる。

【0021】第２のデジタルデータ管理システムはネットワーク上のデータ管理センタ、原著作権者あるいは情

報提供者とネットワークを利用する複数のユーザから構成されている。データ管理センタはネットワーク利用者の公開鍵の認証と原データ及び加工シナリオの保管を行うとともにユーザラベル原データラベル及び加工データラベルの保管を行う。ユーザ間ではデータは転送されず、公開鍵で暗号化されたデータラベルが転送される。転送及び利用申込みにはデータラベルが使用されるが、代わりにデータラベルの電子指紋を使用することもできる。

【００２２】電子商取引システムでは、すべてのデータがネットワーク上の仲介業者を介して流通し、生産者から需要者に転送されるデータは暗号化用秘密鍵で暗号化され、需要者から生産者に転送されるデータは再暗号化用秘密鍵で暗号化される。

【００２３】

【実施例】本発明の実施例として、第１実施例～第５実施例を説明するが、初めにこれらの実施例に共通する基本的事項について説明する。

【認証機関】本発明では、原著作物の著作権所有者、原著作物の提供者（Infomation Provider：ＩＰ）、原著作物の利用者、原著作物の加工者の認証を行うための機関が必要である。この機関は唯一のものであってもよいが、複数の機関が存在してもよい。複数の機関が存在場合には、それらをリンクさせることにより仮想的に１つの機関であるとみなせるようにすることもできる。

【００２４】また、このシステムにおいて、各利用者の公開鍵－専用鍵のセット及び著作物が使用される段階毎に異なる秘密鍵が使用される。これらの中、専用鍵は各利用者が自らの責任において管理し、対応する公開鍵に認証機関がデジタル署名を行うことにより、信頼性を確保する。この公開鍵は一般的にはキーライブラリと称される鍵管理機関が管理し、利用者の要求に応じて配布されるが、認証機能を有する機関を鍵管理機関とリンクさせ、あるいは認証機能を有する機関が鍵管理機関の機能を兼ね備えるようにすることもできる。

【００２５】【暗号鍵】使用される鍵システム及びデジタル署名システムについて簡単に説明する。秘密鍵(secret key)システムは暗号化と復号化が同じ鍵で行われるため「共通鍵システム」とも呼ばれ、鍵を秘密にしておく必要があることから「秘密鍵システム」と呼ばれる。秘密鍵を用いる暗号アルゴリズムとして代表的なものに米国標準局(National Bureau of Standards)のＤＥＳ(Data Encryption Standard)システム，日本電信電話のＦＥＡＬ(Fast Encryption Algorithm)システム，三菱電機のＭＩＳＴＹシステムがある。以下説明する実施例において秘密鍵を「Ｋs」と表示する。

【００２６】これに対して公開鍵システムは、公開されている公開鍵(public key)とその鍵の所有者以外には秘密にされている専用鍵(private key)を用い、一方の鍵で暗号化し他方の鍵で復号化する暗号システムであり、代表的なものにＲＳＡ公開鍵システムがある。以下説明する実施例において公開鍵を「Ｋb」と、専用鍵を「Ｋv」と表示する。このときに、データＭ(Material)を暗号鍵Ｋを用いた暗号Ｃk(Cryptgram)に暗号化(Encryption)する操作を、

Ｃk＝Ｅ（Ｍ．Ｋ）

暗号Ｃkを暗号鍵Ｋを用いてデータＭに復号化(Decryption)する操作を、

Ｍ＝Ｄ（Ｃk　Ｋ）

と表現する。

【００２７】デジタル署名は公開鍵システムを応用した技術であり、転送元がデータＭを例えばＭＤ５等の一方向ハッシュ関数によってハッシュ値Ｈmとし、そのハッシュ値Ｈmを専用鍵Ｋvを用いてＣhmkvに暗号化してデータＭとともに転送先に転送し、転送先は転送された暗号化ハッシュ値Ｃhmkvを公開鍵Kbを用いてハッシュ値Ｈmに復号化するとともに転送されたデータＭを同じ一方向ハッシュ関数によってハッシュ値Ｈm'とし、Ｈm＝Ｈm'であれば転送されたデータが信頼できると判定するシステムである。なお、この過程で得られるハッシュ値Ｈmはデータから１意的に求められ、且つハッシュ値Ｈmからデータを１意的に再現することは不可能である。また、転送元と転送先が相互を確認できる場合にはハッシュ値Ｈmを暗号化することなく転送した場合であっても転送データの信頼性は確保されるため、電子指紋(electronic fingerprinting)と呼ばれ、簡易認証に用いられる。

【００２８】【鍵の使用】第１実施例～第５実施例では、センタ側装置以外の装置においてデータの暗号化／復号化／再暗号化処理，データの保存禁止処理及び暗号鍵の保管が行われるが、これらの操作は自動的に動作する専用のアプリケーションプログラム，データに内蔵されるアプリケーションプログラムあるいはより安全性を高くするためにはオペレーティングシステムによって行われるのが望ましい。また、これらの処理をＩＣカードあるいはＰＣカード等を用いて行うことにより、より高度の安全性を得ることができる。

【００２９】【課金】データの使用に応じた課金を確実に行う方法としては、使用の前に使用見込みに応じた課金を行う方法と、使用後に使用実績に応じた課金を行う方法がある。また、使用後に課金を行う方法には、使用実績を記録しておき後で使用記録を調べて課金するメータリング後払い方式と、予め購入金額が記入されたカード等を用いて使用実績に応じて記入金額が減額されるカード前払い方式がある。さらに、メータリング後払い方式には記録装置がサーバ側に設置されている電話料金方式と、記録装置がユーザ端末装置側に設置されている電気料金方式がある。また、カード前払い方式にも前払いカードがサーバ側に保管されているクレジットカード方式と、前払いカードがユーザ側に保管されているプリペ

イドカード方式がある。

【0030】第1実施例～第4実施例では、ユーザがシステムを利用することを登録するときに提示するユーザ情報に基づき、データ管理センタがユーザラベルを作成し、ユーザに送信し、ユーザはユーザラベル及びシステムにおいて使用するユーザ公開鍵、ユーザ専用鍵、データ管理センタの公開鍵を自らの装置内に保管しておく。これらの保管場所としては、ＩＣカードあるいはＰＣカードが最適であるが、装置内のデータ保存装置内に保管しておくこともできる。ＩＣカードあるいはＰＣカードによる暗号鍵保管方法はオペレーティングシステムによる鍵管理よりも高い安全性を確保することができる。

【0031】以下説明する実施例は、デジタルデータ著作権を管理するシステムについて説明するが、著作物データ以外にも電子商取引データ，電子通貨データ等通信内容、取引内容等秘匿性、確実性、信頼性を要求されるデジタルデータがあり、これらのデジタルデータに対しても本発明が適用可能である。また、暗号鍵を使用するネットワークシステムにおいて暗号鍵を保管する機関及び暗号鍵を生成する機関はネットワークシステムの外に置かれネットワークシステムを経由して利用されるが、以下説明する実施例においては、説明を単純化させるために唯一の機関、すなわちデータ管理センタ、がこれら全ての機関を兼ねているとして説明する。

【0032】［ラベル］本発明では、データの著作権を保護し、データ著作権を行使するためにラベルを利用するので、初めにラベルについて図1，図2及び図3を用いて説明する。このシステムにおいて、システム利用者のユーザラベルが使用されるが、ユーザラベルには図1（a）に示すようにラベル所有者の情報が記載されている。さらにラベル所有者が原著作権を有する場合には図1（b）に示すように原著作物に関する情報が付加されており，その著作物が原著作物を加工して得られた加工著作物である場合には図1（c）に示すように原著作権データに関する情報，加工ツールの情報及び加工データ（加工シナリオ）がさらに付加されており，図1（d）に示すように加工ツール情報の代わりに加工ツール（加工プログラム）を付加することもできる。これらのラベル中、図1（a）に示されたラベル所有者の情報のみが記載されたラベルを「ユーザラベル」と呼び、図1（b）に示された著作物の情報が記載されたラベルを「著作権ラベル」と呼び、さらに図1（c）及び図1（d）に示された加工シナリオが記載されたラベルを「加工ラベル」と呼ぶ。

【0033】ユーザラベルは利用者がシステムに加入するときに利用者の情報に基づきデータ管理センタにより生成され、著作権ラベルは著作を行った著作者がデータ管理センタにその内容を提示することによりデータ管理センタによって生成され、加工ラベルはデータの加工を行った利用者がユーザラベルと加工シナリオをデータ管理センタに提示することによりデータ管理センタによって作成され、これらは各々のラベル所有者に転送されるとともに、データ管理センタ内に保存される。

【0034】［暗号化の対象］図2（a），図2（b），図2（c）に著作権ラベルと著作物データとの関係を示す。著作権ラベルとラベルが対応する著作物データは、図2（a）に示したように著作物データのヘッダと切り放されている場合と、図2（b）に示したように著作物データのヘッダとは一体化している場合と、図2（c）に示したように著作権ラベルがヘッダと結合している場合がある。著作権ラベルがヘッダと結合している場合には、図2（d）に示したように複数の著作権ラベルを組み合わした拡張ラベル構成を行うことができる。図2（b）に示された一体化されたラベルの場合に、著作権ラベルが大きくなると容量に制限のある単一のヘッダにラベルが収納しきれない場合があり、図2（d）に示された複数のラベルを組み合わせた拡張ラベル構成が採られた場合に同様にラベルの数が多くなりすぎるとインターネット上でのパケットの大きさ制限を越え、流通が困難になる場合がある。

【0035】著作権ラベルは、図3（a）に示したように暗号化されて使用される場合と、図3（b）に示したように暗号化されずに使用される場合がある。これらの図において４角枠部分が暗号化される部分である。なお、著作権ラベルが暗号化されない場合には著作物データが暗号化される。著作権ラベルが暗号化されない場合であっても図2（d）に示された拡張ラベル構成において、最後に付加された著作権ラベル以外の著作権ラベルが暗号化され、図3（c）及び図3（d）に示したように、後で付加された著作権ラベル中にその前に付加され暗号化された著作権ラベルの暗号鍵が含まれている多段構成を採用することができ、この構成により前に付加された著作権ラベルの内容を確認することができる。

【0036】著作権保護のためにデータの暗号化／復号化が行われるが、暗号化／復号化はコンピュータにとってかなり負担が大きい作業である。暗号化／復号化の対象となるデータが文字を主体としたテキストデータである場合には暗号化／復号化の作業負担はそれほどでもないが、対象とするデータが音声データ，画像データ，中でも動画データである場合の暗号化／復号化の作業量は膨大なものになる。そのため、高速の暗号アルゴリズムを用いた場合でも、超並列型スーパーコンピュータ等の特殊なコンピュータを使用する場合を除いて、一般的に使用されているパーソナルコンピュータによってテキストデータ以外のデータ、例えば動画像データ，をリアルタイムに暗号化／復号化することは、現段階では実用的ではない。

【0037】図4（a），図4（b），図4（c），図4（d），図4（e），図4（f）及び図4（g）によりデータの暗号化／復号化構成について説明する。これ

らの図において４角枠の部分が暗号化される部分である。図４（ａ）に示したのは、原理的な暗号の使用法であり、ヘッド部と比較して圧倒的に大きいデータボディ部のみが暗号化され、データを認識するために用いられるデータヘッダ部は暗合されていない。このような構成の場合には暗号化／復号化の作業負担が非常に大きくなる。

【００３８】これに対して、図４（ｂ）に示したようにデータボディ部は暗号化せずデータヘッダ部を暗号化する方法がある。この場合ヘッダを全て暗号化してしまうとデータを認識することができなくなるため、ヘッダの一部が暗号化されていない。

【００３９】図４（ａ）に示された構成の作業負担を軽減するための方法として図４（ｃ）に示したように暗号化されるデータボディをその先頭部分だけにすることができる。この構成によれば、暗号化／復号化する必要があるのはデータボディの極く一部だけであるから、暗号化／復号化の作業負担は著しく軽減される。

【００４０】図４（ｄ）に示したのは図４（ｃ）の構成による効果がより高くなるようにしたものであって、データボディ中の暗号化部をデータボディ中に複数設けたものである。

【００４１】図４（ｅ）に示したのは、ＳＫＩＰ(Simple Key-management for Internet Protcols)とよばれる方法であり、データボディが暗号化されるとともにヘッダの一部が暗号化され、ヘッダ中の暗号化部分にデータボディ復号用の暗号鍵がおかれている。この構成によれば、暗号解読は２つの暗号を解読しなければならないため著しく困難である。

【００４２】しかし、図４（ｅ）に示された構成の場合データボディ部全体が暗号化されるため図４（ｅ）に示された構成の場合と同様に、暗号化／復号化の作業負担が非常に大きい。このことへの対応として、図４（ｅ）に示された構成に図４（ｃ）に示された構成を組み合わせて暗号化されるデータボディをその先頭部分だけにし図４（ｆ）のように構成すれば、暗号化／復号化する必要があるのはデータボディの極く一部だけであるから、暗号化／復号化の作業負担は著しく軽減される。

【００４３】図４（ｅ）に示された構成は、さらに図４（ｄ）に示された構成と組み合わせて図４（ｇ）に示されたように、データボディ中の暗号化部をデータボディ中に複数設けた構成とすることにより、効果がより高くなる。

【００４４】図５（ａ）．図５（ｂ）及び図５（ｃ）により通常のファイル形式を有するデータの暗号化／復号化構成について説明する。これらの図において４角枠の部分が暗号化される部分である。通常のファイル形式を有するデータは、データボディ部とデータヘッダ部から構成され、本発明においてはさらに付属しあるいは関連する著作権ラベルから構成されている。図５（ａ）に示したのは、原理的な暗号の使用法であり、著作権ラベル及びデータヘッダ部は暗合されておらずデータボディ部のみが暗号化されており、図４（ａ）の場合と同様に暗号化／復号化の作業負担が非常に大きい。

【００４５】これに対して、図５（ｂ）に示したようにデータボディ部は暗号化せずデータヘッダ部を暗号化する方法がある。この場合ヘッダを全て暗号化してしまうとデータを認識することができなくなるため、ヘッダの一部が暗号化されていない。なお、この場合著作権ラベルも暗号化されていない。

【００４６】また、図５（ｃ）に示したようにデータボディ部及びデータヘッダ部は暗号化せず、著作権ラベルを暗号化する方法がある。なお、この場合も著作権ラベルを全て暗号化してしまうと著作権ラベルと対応するデータとの関係が不明になるため、著作権ラベルの一部が暗号化されていない。

【００４７】一方、データヘッダとデータボディから構成される通常の形式のファイルの代わりに、データとデータを扱うプログラムとが一体化された「オブジェクト」を用いて種々の処理を行う「オブジェクト指向プログラミング(object oriented programing)」がある。オブジェクトは図６（ａ）に示した基本的概念構造を有しており、インスタンス(instance)と呼ばれる容器(envelope)中のスロット(slot)と呼ばれる格納箇所にインスタンス変数(instance variable)と呼ばれるデータが格納され、スロットの周囲は参照(refering)用，加工(processing)用，結合(binding)用等の１個又は複数のメソッド(method)と呼ばれる手続きで包囲されており、インスタンス変数を参照したり操作したりすることはメソッドを介してしか行うことはできず、この機能は隠蔽(encapsulation)と呼ばれる。また、インスタンス変数の参照あるいは操作をメソッドに行わせる外部からの命令をメッセージと呼ぶ。

【００４８】このことは見方を変えると、メソッドを介さなければ参照あるいは操作することができないインスタンス変数はメソッドによって保護されていることになる。このことを利用し、図６（ｂ）に示すように、メソッドを暗号化し、暗号化されたメソッドを復号できるメッセージでなければインスタンス変数を参照あるいは操作することができないようにすることができる。この場合も図５（ｃ）に示された通常のファイル形式を有するデータの場合と同様にメソッドの全てを暗号化してしまうとオブジェクトを利用することができなくなるため、メソッドの一部を暗号化しない。なお、４角枠の部分が暗号化された部分である。

【００４９】［第１実施例］図７により、第１実施例を説明する。原理的な説明を行うために、ユーザが原著作物データを加工することなく、次のユーザに転送する場合について説明するが、ユーザが原著作物データの加工を行う場合については、後に説明する。なお、実際には

原著作物データの加工が行われない場合と、後に示す第３実施例で説明する原著作物データの加工が行われる場合が組み合わされて実施される。なお、この実施例のシステムにおいては秘密鍵及び公開鍵一専用鍵が使用される。したがって、データ管理センタに公開鍵管理機関及び秘密鍵生成機関がリンクされあるいは含まれることがある。

【００５０】(1) 原著作者（データ所有者）Ａは、原著作権ラベルＬｏを提示して、原秘密鍵Ｋｓｏの配布を、データ管理センタＣｄに要求する。なお、原著作者が、情報提供業者（ＩＰ）あるいはデータベースに原著作物データを譲渡あるいは管理預託しておき、情報提供業者（ＩＰ）あるいはデータベースが原著作者の役割を果たすようにすることもできる。また、原著作者Ａが原秘密鍵Ｋｓｏを保管し、データ管理センタＣｄに依存することなく原著作物データＭｏの暗号化を行うことも可能であるが、ユーザ（データ利用者）による原著作物データＭｏの利用を行うためにはデータ管理センタＣｄに原秘密鍵Ｋｓｏが保管されている必要がある。

【００５１】(2) 原秘密鍵Ｋｓｏの配布を要求されたデータ管理センタＣｄは、原著作権ラベルＬｏとともに原著作権ラベルＬｏに対応させた原秘密鍵Ｋｓｏを原著作者Ａの公開鍵Ｋｂａを用いて暗号化し、

Ｃｄｓｏｋｂａ＝Ｅ（Ｋｓｏ，Ｋｂａ）

暗号化原秘密鍵Ｃｋｓｏｋｂａを、原著作者Ａに配付する。以降、秘密鍵は配付先でのみ復号可能なように配付先の公開鍵を用いて暗号化されて配布される。

【００５２】データ管理センタＣｄは、このときに原著作権ラベルＬｏをＭＤ５(Message Digest 5)等のアルゴリズムを用いて一方向ハッシュを行い、原著作権ラベル指紋Ｆｏ，例えば１６バイトのデータ量を有する、を作成し、原著作者Ａに配布する。以後、この電子指紋は著作物データとともに転送される。

【００５３】(3) 暗号化原秘密鍵Ｃｋｓｏｋｂａを配付された原著作者Ａは、暗号化原秘密鍵Ｃｋｓｏｋｂａを原著作者Ａの専用鍵Ｋｖａを用いて復号し、

Ｋｓｏ＝Ｄ（Ｃｋｓｏｋｂａ，Ｋｖａ）

復号された原秘密鍵Ｋｓｏを用いて原著作物データＭｏを暗号化し、

Ｃｍｏｋｓｏ＝Ｅ（Ｍｏ，Ｋｓｏ）

暗号化原著作物データＣｍｏｋｓｏと原著作権ラベルＬｏ及び原著作権ラベル指紋Ｆｏを、第１ユーザ（最初のデータ利用者）Ｕ1に転送する。

【００５４】(4) 暗号化原著作物データＣｍｏｋｓｏと原著作権ラベルＬｏ及び原著作権ラベル指紋Ｆｏを転送された第１ユーザＵ1は、原著作権ラベルＬｏと原著作権ラベル指紋Ｆｏ及び第１ユーザラベルＬｕ1を提示して、原秘密鍵Ｋｓｏ及び第１秘密鍵Ｋｓ1の配布を、データ管理センタＣｄに要求する。

【００５５】(5) 原秘密鍵Ｋｓｏ及び第１秘密鍵Ｋｓ1の配布を要求されたデータ管理センタＣｄは、提示された原著作権ラベルＬｏの正当性を原著作権ラベル指紋Ｆｏによって確認して、第１ユーザラベルＬｕ1を登録するとともに、原著作権ラベルＬｏに対応する原秘密鍵Ｋｓｏ及び第１ユーザラベルＬｕ1に対応させた第１秘密鍵Ｋｓ1を第１ユーザＵ1の公開鍵Ｋｂ1を用いて暗号化して、

Ｃｋｓｏｋｂ1＝Ｅ（Ｋｓｏ，Ｋｂ1）

Ｃｋｓ1ｋｂ1＝Ｅ（Ｋｓ1，Ｋｂ1）

暗号化原秘密鍵Ｃｋｓｏｋｂ1及び暗号化第１秘密鍵Ｃｋｓ1ｋｂ1を、第１ユーザＵ1に配布する。

【００５６】(6) 暗号化原秘密鍵Ｃｋｓｏｋｂ1及び暗号化第１秘密鍵Ｃｋｓ1ｋｂ1を配布された第１ユーザＵ1は、暗号化原秘密鍵Ｃｋｏｋｂ1及び暗号化第１秘密鍵Ｃｋｓ1ｋｂ1を第１ユーザＵ1の専用鍵Ｋｖ1を用いて復号し、

Ｋｓｏ＝Ｄ（Ｃｋｓｏｋｂ1，Ｋｖ1）

Ｋｓ1＝Ｄ（Ｃｋｓ1ｋｂ1，Ｋｖ1）

復号された原秘密鍵Ｋｓｏを用いて暗号化原著作物データＣｍｏｋｓｏを復号し、

Ｍｏ＝Ｄ（Ｍｏ，Ｋｓｏ）

復号された原著作物データＭｏを利用する。

【００５７】原著作物データＭｏを保存，複写する場合には、復号された第１秘密鍵Ｋｓ1を用いて暗号化し、

Ｃｍｏｋｓ1＝Ｅ（Ｍｏ，Ｋｓ1）

暗号化原著作物データＣｍｏｋｓ1として保存，複写し、原著作物データＭｏを第２ユーザ（次のデータ利用者）Ｕ2に転送する場合には、復号された第１秘密鍵Ｋｓ1を用いて暗号化し、暗号化原著作物データＣｍｏｋｓ1として原著作権ラベルＬｏ，原著作権ラベル指紋Ｆｏ及び第１ユーザラベルＬｕ1とともに、転送する。

【００５８】なお、各ユーザが、データ管理センタＣｄに提示するそのユーザのラベルにそのラベルの一方向性ハッシュ値をユーザの専用鍵を用いて暗号化したデジタル署名を付け、データ管理センタがそのユーザの公開鍵を用いて暗号化一方向性ハッシュ値を復号し、そのラベルの一方向性ハッシュ値を計算し、両一方向性ハッシュ値を比較することにより、各ユーザラベルの正当性の検証を行うことができる。

【００５９】(7) 暗号化原著作物データＣｍｏｋｓ1，原著作権ラベルＬｏ，原著作権ラベル指紋Ｆｏ及び第１ユーザラベルＬｕ1を転送された第２ユーザＵ2は、原著作権ラベルＬｏ，原著作権ラベル指紋Ｆｏ及び第１ユーザラベルＬｕ1及び第２ユーザラベルＬｕ2を提示して、第１秘密鍵Ｋｓ1及び第２秘密鍵Ｋｓ2の配布を、データ管理センタＣｄに要求する。

【００６０】(8) 第１秘密鍵Ｋｓ1及び第２秘密鍵Ｋｓ2の配布を要求されたデータ管理センタＣｄは、原著作権ラベル指紋Ｆｏによって原著作権ラベルＬｏ及び第１ユーザラベルＬｕ1の正当性を確認する。第１ユーザラベルＬｕ1が正当なものであることが確認されると、データ管理センタＣｄは、第２ユーザラベルＬｕ2を登録し、第１ユー

ザラベルLu1に対応する第1秘密鍵Ks1及び第2ユーザラベルLu2に対応させた第2秘密鍵Ks2を各々第2ユーザの公開鍵Kb2を用いて暗号化し、

Cks1kb2＝E（Ks1，Kb2）

Cks2kb2＝E（Ks2，Kb2）

暗号化第1秘密鍵Cks1kb2及び暗号化第2秘密鍵Cks2kb2を、第2ユーザU2に配付する。

【0061】(9) 暗号化第1秘密鍵Cks1kb2及び暗号化第2秘密鍵Cks2kb2を配付された第2ユーザU2は、暗号化第1秘密鍵Cks1kb2及び暗号化第2秘密鍵Cks2kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

Ks1＝D（Cks1kb2，Kv2）

Ks2＝D（Cks2kb2，Kv2）

復号された第1秘密鍵Ks1を用いて暗号化原著作物データCm0ks1を復号し、

M0＝D（Cm0ks1，Ks1）

復号された原著作物データM0を利用する。

【0062】原著作物データM0を保存，複写する場合には、復号された第2秘密鍵Ks2を用いて暗号化し、暗号化原著作物データCm0ks2が保存，複写され、原著作物データM0を第3ユーザU3に転送する場合には、復号された第2秘密鍵Ks2を用いて暗号化し、暗号化原著作物データCm0ks2を原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1及び第2ユーザラベルLu2とともに、第3ユーザU3に転送する。

【0063】(10) 暗号化原著作物データCm0ks2を原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1及び第2ユーザラベルLu2とともに転送された第3ユーザU3は、原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1，第2ユーザラベルLu2及び第3ユーザラベルLu3を提示して第2秘密鍵Ks2及び第3秘密鍵Ks3の配布を、データ管理センタCdに要求する。

【0064】(11) 第2秘密鍵Ks2及び第3秘密鍵Ks3の配布を要求されたデータ管理センタCdは、原著作権ラベル指紋F0によって、原著作権ラベルL0，第1ユーザラベルLu1及び第2ユーザラベルLu2が正当なものであるか否かを確認する。第2ユーザラベルLu2が正当なものであることが確認されると、データ管理センタCdは、第3ユーザラベルLu3を登録し、第2ユーザラベルLu2に対応する第2秘密鍵Ks2及び第3ユーザラベルLu3に対応させた第3秘密鍵Ks3を各々第3ユーザU3の公開鍵Kb3を用いて暗号化して、

Cks2kb3＝E（Ks2，Kb3）

Cks3kb3＝E（Ks3，Kb3）

暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb3を、第3ユーザU3に配付する。

【0065】(12) 暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb3を配付された第3ユーザU3は、暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb3を第3ユーザU3の専用鍵Kv3を用いて復号し、

Ks2＝D（Cks2kb3，Kv3）

Ks3＝D（Cks3kb3，Kv3）

復号された第2秘密鍵Ks2を用いて暗号化原著作物データCm0ks2を復号し、

M0＝D（Cm0ks2，Ks2）

復号された原著作物データM0を利用する。

【0066】原著作物データM0を保存，複写する場合には、復号された第3秘密鍵Ks3を用いて暗号化し、暗号化原著作物データCm0ks3が保存，複写され、原著作物データM0を第4ユーザU4に転送する場合には、復号された第3秘密鍵Ks3を用いて暗号化し、暗号化原著作物データCm0ks3が原著作権ラベルL0，第1ユーザラベルLu1，第2ユーザラベルLu2及び第3ユーザラベルLu3とともに、第4ユーザU4に転送される。以後、同様な動作が繰り返される。

【0067】［第2実施例］著作物データを暗号化するために用いられる鍵が著作物データを復号化するために用いられる鍵とは別に送付される第2実施例を図8により説明する。なお、この第2実施例における鍵の取り扱い，原著作者，情報提供者，ユーザの関係，ラベルの取り扱いは、第1実施例の場合と同様なので、再度説明することは省略する。

【0068】(1) 原著作者Aは、原著作権ラベルL0を提示して、原秘密鍵Ks0の配布を、データ管理センタCdに要求する。

【0069】(2) 原秘密鍵Ks0の配布を要求されたデータ管理センタCdは、原著作権ラベルL0から原著作権ラベル指紋F0を作成し、原著作権ラベルL0とともに原著作権ラベルL0に対応させた原秘密鍵Ks0を原著作者Aの公開鍵Kbaを用いて暗号化し、

Cks0kba＝E（Ks0，Kba）

暗号化原秘密鍵Cks0kbaを、原著作者Aに配付する。

【0070】(3) 暗号化原秘密鍵Cks0kbaを配付された原著作者Aは、暗号化原秘密鍵Cks0kbaを原著作者Aの専用鍵Kvaを用いて復号し、

Ks0＝D（Cks0kba，Kva）

復号された原秘密鍵Ks0を用いて原著作物データM0を暗号化し、

Cm0ks0＝E（M0，Ks0）

暗号化原著作物データCm0ks0と原著作権ラベルL0及び原著作権ラベル指紋F0を、第1ユーザU1に転送する。

【0071】(4) 暗号化原著作物データCm0ks0と原著作権ラベルL0及び原著作権ラベル指紋F0を転送された第1ユーザU1は、原著作権ラベルL0と原著作権ラベル指紋F0及び第1ユーザラベルLu1を提示して、原秘密鍵Ks0の配布を、データ管理センタCdに要求する。

【0072】(5) 原秘密鍵Ks0の配布を要求されたデータ管理センタCdは、提示された原著作権ラベルL0の正当性を原著作権ラベル指紋F0によって確認して、第1

ユーザラベルLu1を登録するとともに、原著作権ラベルL0に対応する原秘密鍵Ks0を第1ユーザU1の公開鍵Kb1を用いて暗号化して、

Cks0kb1＝E（Ks0, Kb1)

暗号化原秘密鍵Cks0kb1を、第1ユーザU1に配布する。

【0073】(6) 暗号化原秘密鍵Cks0kb1を配布された第1ユーザU1は、暗号化原秘密鍵Ck0kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

Ks0＝D（Cks0kb1, Kv1)

復号された原秘密鍵Ks0を用いて暗号化原著作物データCm0ks0を復号し、

M0＝D（M0, Ks0)

復号された原著作物データM0を利用する。

【0074】(7) 原著作物データM0を保存，複写する場合には、再度原著作権ラベルL0と原著作権ラベル指紋F0及び第1ユーザラベルLu1を提示して、第1秘密鍵Ks1の配布を、データ管理センタCdに要求する。

【0075】(8) 第1秘密鍵Ks1の配布を要求されたデータ管理センタCdは、提示された第1ユーザラベルLu1の正当性を原著作権ラベル指紋F0によって確認して、登録された第1ユーザラベルLu1に対応させた第1秘密鍵Ks1を第1ユーザU1の公開鍵Kb1を用いて暗号化して、

Cks1kb1＝E（Ks1, Kb1)

暗号化第1秘密鍵Cks1kb1を、第1ユーザU1に配布する。

【0076】(9) 暗号化第1秘密鍵Cks1kb1を配布された第1ユーザU1は、暗号化第1秘密鍵Cks1kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

Ks1＝D（Cks1kb1, Kv1)

原著作物データM0を復号された第1秘密鍵Ks1を用いて暗号化し、

Cm0ks1＝E（M0, Ks1)

暗号化原著作物データCm0ks1として保存，複写し、原著作物データM0を第2ユーザU2に転送する場合には、復号された第1秘密鍵Ks1を用いて暗号化し、暗号化原著作物データCm0ks1として原著作権ラベルL0，原著作権ラベル指紋F0及び第1ユーザラベルLu1とともに、転送する。

【0077】(10) 暗号化原著作物データCm0ks1，原著作権ラベルL0，原著作権ラベル指紋F0及び第1ユーザラベルLu1を転送された第2ユーザU2は、原著作権ラベルL0，原著作権ラベル指紋F0及び第1ユーザラベルLu1及び第2ユーザラベルLu2を提示して、第1秘密鍵Ks1の配布を、データ管理センタCdに要求する。

【0078】(11) 第1秘密鍵Ks1の配布を要求されたデータ管理センタCdは、原著作権ラベル指紋F0によって原著作権ラベルL0及び第1ユーザラベルLu1の正当性を確認する。第1ユーザラベルLu1が正当なものであることが確認されると、データ管理センタCdは、第2ユーザラベルLu2を登録し、第1ユーザラベルLu1に対応する第1秘密鍵Ks1を各々第2ユーザの公開鍵Kb2を用いて暗号化し、

Cks1kb2＝E（Ks1, Kb2)

暗号化第1秘密鍵Cks1kb2を、第2ユーザU2に配付する。

【0079】(12) 暗号化第1秘密鍵Cks1kb2を配付された第2ユーザU2は、暗号化第1秘密鍵Cks1kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

Ks1＝D（Cks1kb2, Kv2)

復号された第1秘密鍵Ks1を用いて暗号化原著作物データCm0ks1を復号し、

M0＝D（Cm0ks1, Ks1)

復号された原著作物データM0を利用する。

【0080】(13) 原著作物データM0を保存，複写する場合には、再度原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1及び第2ユーザラベルLu2を提示して、第2秘密鍵Ks2の配布を、データ管理センタCdに要求する。

【0081】(14) 第2秘密鍵Ks2の配布を要求されたデータ管理センタCdは、提示された第2ユーザラベルLu2の正当性を原著作権ラベル指紋F0によって確認して、登録された第2ユーザラベルLu2に対応させた第2秘密鍵Ks2を第2ユーザU2の公開鍵Kb2を用いて暗号化して、

Cks2kb2＝E（Ks2, Kb2)

暗号化第2秘密鍵Cks2kb2を、第2ユーザU2に配布する。

【0082】(15) 暗号化第2秘密鍵Cks2kb2を配布された第2ユーザU2は、暗号化第2秘密鍵Cks2kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

Ks2＝D（Cks2kb2, Kv2)

原著作物データM0を復号された第2秘密鍵Ks2を用いて暗号化し、

Cm0ks2＝E（M0, Ks2)

暗号化原著作物データCm0ks2として保存，複写し、原著作物データM0を第3ユーザU3に転送する場合には、復号された第2秘密鍵Ks2を用いて暗号化し、暗号化原著作物データCm0ks2として原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1及び第2ユーザラベルLu2とともに、第3ユーザU3に転送する。

【0083】(16) 暗号化原著作物データCm0ks2を原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1及び第2ユーザラベルLu2とともに転送された第3ユーザU3は、原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1，第2ユーザラベルLu2及び第3ユーザラベルLu3を提示して第2秘密鍵Ks2の配布を、データ管理センタCdに要求する。

【0084】(17) 第2秘密鍵Ks2の配布を要求された

データ管理センタCdは、原著作権ラベル指紋F0によって、原著作権ラベルL0、第1ユーザラベルLu1及び第2ユーザラベルLu2が正当なものであるか否かを確認する。第2ユーザラベルLu2が正当なものであることが確認されると、データ管理センタCdは、第3ユーザラベルLu3を登録し、第2ユーザラベルLu2に対応する第2秘密鍵Ks2を第3ユーザU3の公開鍵Kb3を用いて暗号化して、

Cks2kb3＝E（Ks2，Kb3）

暗号化第2秘密鍵Cks2kb3を、第3ユーザU3に配付する。

【0085】(18) 暗号化第2秘密鍵Cks2kb3を配付された第3ユーザU3は、暗号化第2秘密鍵Cks2kb3を第3ユーザU3の専用鍵Kv3を用いて復号し、

Ks2＝D（Cks2kb3，Kv3）

復号された第2秘密鍵Ks2を用いて暗号化原著作物データCm0ks2を復号し、

M0＝D（Cm0ks2，Ks2）

復号された原著作物データM0を利用する。

【0086】(19) 原著作物データM0を保存，複写する場合には、再度原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1，第2ユーザラベルLu2及び第3ユーザラベルLu3を提示して、第3秘密鍵Ks3の配布を、データ管理センタCdに要求する。

【0087】(20) 第3秘密鍵Ks3の配布を要求されたデータ管理センタCdは、提示された第3ユーザラベルLu3の正当性を原著作権ラベル指紋F0によって確認して、登録された第3ユーザラベルLu3に対応させた第3秘密鍵Ks3を第3ユーザU3の公開鍵Kb3を用いて暗号化して、

Cks3kb3＝E（Ks3，Kb3）

暗号化第3秘密鍵Cks3kb3を、第3ユーザU3に配布する。

【0088】(21) 暗号化第3秘密鍵Cks3kb3を配布された第3ユーザU3は、暗号化第3秘密鍵Cks3kb3を第3ユーザU3の専用鍵Kv3を用いて復号し、

Ks3＝D（Cks3kb3，Kv3）

原著作物データM0を復号された第3秘密鍵Ks3を用いて暗号化し、

Cm0ks3＝E（M0，Ks3）

暗号化原著作物データCm0ks3として保存，複写し、原著作物データM0を第4ユーザU4に転送する場合には、復号された第3秘密鍵Ks3を用いて暗号化し、暗号化原著作物データCm0ks3として原著作権ラベルL0，原著作権ラベル指紋F0，第1ユーザラベルLu1，第2ユーザラベルLu2及び第3ユーザラベルLu3とともに、第4ユーザU4に転送する。以後、同様な動作が繰り返される。

【0089】この実施例の場合には、初めに著作物データの利用に必要な復号用の鍵だけが配布されるため、著作物データの保存，複写あるいは転送を行わない利用者にとっては操作が簡略化される。なお、第1実施例のように再暗号用の鍵が復号用の鍵と同時に配布されるシステムと、第2実施例のように再暗号用の鍵が復号用の鍵と別々に配布されるシステムとを一つのシステム中に共存させ、適宜選択して利用するように構成することも可能である。

【0090】［第3実施例］ユーザが1つの原著作物データを加工して、次のユーザに転送する第3実施例を図9及び図10により説明する。データ著作物の加工は、原著作物データをアプリケーションプログラムである加工ツールを用いて編集することによって行われ、加工によって得られた加工著作物データは、利用した原著作物データ，使用した加工ツールの情報及び加工内容データとによって表現することができる。すなわち、加工ツールを所有している場合には、原著作物データと加工内容データを入手することにより、加工著作物データを再現することが可能である。

【0091】デジタルデータの加工について説明する。デジタルデータの加工は加工用プログラム（加工ツール）を利用して原データに改変を加えることによってなされるため、原データ，加工ツール及び加工内容データ（加工シナリオ）が特定されることによって加工データが再現される。いいかえれば、原データ，加工ツールと加工シナリオが特定されなければ加工データの再現は不可能である。

【0092】単一の原データにより新しいデータを作成する場合には、原データAを改変して加工データ「A'」を得る場合、原データAにユーザがデータXを付加することにより加工データ「A＋X」を得る場合、原データAを原データ要素A1，A2，A3・・・に分割し配列をA3，A2，A1のように変更して加工データ「A"」を得る場合、原データAを原データ要素A1，A2，A3・・・に分割し1次ユーザのデータXをX1，X2，X3・・・に分割しこれらを配列して加工データ「A1＋X1＋A2＋X2＋A3＋X3・・・」を得る場合等がある。これらの場合、原データの改変、原データの配列変更、原データとユーザデータの組み合わせ、原データの分割及びユーザデータとの組み合わせ、が各々二次著作権の対象となり、これらの二次著作権を保護する必要がある。なお、ユーザが付加したデータXにはユーザの原著作権が存在することはいうまでもない。

【0093】複数の原データを組み合わせることにより新しいデータを作成する場合には、原データA，B，C・・・を単純に組み合わせて加工データ「A＋B＋C・・・」を得る場合、原データA，B，C・・・にユーザがデータXを付加することにより加工データ「A＋X」を得る場合、原データA，B，C・・・を原データ要素A1，A2，A3・・・，B1，B2，B3・・・，C1，C2，C3・・・に分割し組み合わせて配列を変更し加工デ

ータ「A1+B1+C1+・・・+A2+B2+C2+・・・+A3+B3+C3+・・・」を得る場合、原データA，B，C・・・を原データ要素A1，A2，A3・・・，B1，B2，B3・・・，C1，C2，C3・・・に分割しユーザのデータX1，X2，X3・・・を組み合わせて配列を変更して加工データ「A1+B1+C1+X1+・・・+A2+B2+C2+X2+・・・+A3+B3+C3+X3+・・・」を得る場合等がある。これらの場合も、複数の原データの組み合わせ、複数の原データとユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された複数の原データとユーザデータの組み合わせ、が各々2次的著作権の対象となり、これらの2次的著作権を保護する必要がある。また、ユーザが付加したデータX1，X2，X3・・・にはユーザの原著作権が存在することはいうまでもない。

【0094】図9に示されたのは複数の原データA，B，Cを利用して新しいデータDを作成する手法例である。この手法は原データA，B，Cから要素a，b，cを抽出（カット）し、抽出された要素a，b，cを貼り付けて（ペースト）1つのデータDを合成するカットアンドペースト手法によってデータの加工を行うものである。

【0095】この他に複数のデータオブジェクトをリンクさせるデータリンク技術がある。このデータリンク技術は、データオブジェクトであるパッド(pad)のスロットにオブジェクトリンク部を設け、このスロットで他のパッドとリンクさせるスロットコネクション(slot connection)技術によりオブジェクト同士をリンクさせる。このようにしてリンクされた複数のオブジェクトの相互関係はツリー構造として表現することができ、さらに表現されたツリー構造を利用してオブジェクトの削除あるいは追加が可能となる。

【0096】ところで、原データ及びユーザデータがデータであることは明白であるが、データの加工過程である原データの改変，原データの配列変更，原データとユーザデータの組み合わせ，原データの分割及びユーザデータとの組み合わせ，複数の原データの組み合わせ，複数の原データとユーザデータの組み合わせ，複数の原データの分割及び配列変更，分割された複数の原データとユーザデータの組み合わせもデータそのものである。

【0097】原データの配置関係及び加工手順等であるデータの加工シナリオもデータであることに着目すると、加工データに関する二次的著作権を原データに関する原著作者の原著作権及びユーザデータに関するユーザの著作権に加えて加工過程データに関するユーザの著作権を管理することによって保護することが可能となる。

【0098】すなわち、加工データを原データとユーザデータと加工シナリオとから構成するものとし、これらの原データ，ユーザデータ及び加工シナリオを管理することにより、原データとともに加工データの著作権を管理することができる。なお、この場合データの加工において使用された加工用プログラムも必要ならばデータ管理システムの管理対象とする。

【0099】このデータの加工は原データをその原データに対応する加工プログラムを使用して加工することもできるが、原データを最近注目されているオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータの合成を行うことができる。

【0100】エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、ユーザ端末装置に装備されたメータリング機能を利用して利用データ明細、課金情報などを含む情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データと同様に暗号化される。

【0101】図10に示された第3実施例においては、先に示した第1実施例及び第2実施例における著作権ラベルに加工シナリオを付加したものを「加工ラベル」と呼び、第1実施例における著作権ラベルと同様に扱う。なお、この第3実施例における鍵の取り扱い、原著作者，情報提供者，ユーザの関係，ラベルの取り扱いも、第1実施例の場合と同様なので、再度説明することは省略する。

【0102】(1) 原著作者Aは、原著作権ラベルL0を提示して、原秘密鍵Ks0の配布を、データ管理センタCdに要求する。

【0103】(2) 原秘密鍵Ks0の配布を要求されたデータ管理センタCdは、原著作権ラベルL0とともに原著作権ラベルL0に対応させた原秘密鍵Ks0を原著作者Aの公開鍵Kbaを用いて暗号化し、

Cds0kba＝E（Ks0，Kba）

暗号化原秘密鍵Cks0kbaを、原著作者Aに配付する。

【0104】データ管理センタCdは、このときに原著作権ラベルL0をMD5等のアルゴリズムを用いて一方向ハッシュ、例えば16バイトのデータ量に、を行い原著作権ラベル指紋F0を作成し、原著作者Aに配布する。この、電子指紋は原著作物あるいは加工が行われ加

工著作物が得られる度に各々の加工著作物について作成され、著作物とともに転送される。

【0105】(3) 暗号化原秘密鍵Cks0kbaを配付された原著作者Aは、暗号化原秘密鍵Cks0kbaを原著作者Aの専用鍵Kvaを用いて復号し、

Ks0=D（Cks0kba, Kva)

復号された原秘密鍵Ks0を用いて原著作物データM0を暗号化し、

Cm0ks0=E（M0, Ks0)

暗号化原著作物データCm0ks0と原著作権ラベルL0及び原著作権ラベル指紋F0を、第1ユーザU1に転送する。

【0106】(4) 暗号化原著作物データCm0ks0と原著作権ラベルL0及び原著作権ラベル指紋F0を転送された第1ユーザU1は、原著作権ラベルL0と原著作権ラベル指紋F0及び第1ユーザラベルLu1を提示して、原秘密鍵Ks0の配布を、データ管理センタCdに要求する。

【0107】(5) 原秘密鍵Ks0の配布を要求されたデータ管理センタCdは、提示された原著作権ラベルL0の正当性を原著作権ラベル指紋F0によって確認して、第1ユーザラベルLu1を登録するとともに、原著作権ラベルL0に対応する原秘密鍵Ks0を第1ユーザU1の公開鍵Kb1を用いて暗号化して、

Cks0kb1=E（Ks0, Kb1)

暗号化原秘密鍵Cks0kb1を、第1ユーザU1に配布する。

【0108】(6) 暗号化原秘密鍵Cks0kb1を配布された第1ユーザU1は、暗号化原秘密鍵Ck0kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

Ks0=D（Cks0kb1, Kv1)

復号された原秘密鍵Ks0を用いて暗号化原著作物データCm0ks0を復号し、

M0=D（M0, Ks0)

復号された原著作物データM0を加工ツールを用いて加工し、加工著作物データMe1を得る。

【0109】このようにして得られた加工著作物データMe1にはデータの加工を行った第1ユーザの著作権とともに、原著作物を作成した原著作者の著作権も存在している。原著作物データM0に関する原著作者の著作権は登録された原著作権ラベルL0及び原著作権ラベル指紋F0と原著作権ラベルL0に対応させた原秘密鍵Ks0、第1ユーザラベルLu1と第1ユーザラベルLu1に対応させた第1秘密鍵Ks1によって保護することができるが、加工著作物データMe1を暗号化する鍵は用意されていないため、加工著作物データMe1に関する第1ユーザの二次著作権は未だ保護される状態にはなっていない。

【0110】(7) 加工著作物データMe1に関する第1ユーザの二次著作権を保護するために、第3実施例においては、加工著作物の著作者である第1ユーザラベルとその電子指紋を利用する。前に説明したように加工著作物は、利用した原著作物データ、使用した加工ツールの情報及び加工内容データとによって表現することができるから、第1ユーザラベルいいかえれば第1加工ラベルLe1にはこれらの情報及びデータが記入される。さらに、以後の流通過程における二次著作権保護のために、ユーザU1は第1加工ラベルLe1を、データ管理センタCdに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【0111】(8) 第1加工ラベルLe1を提示されたデータ管理センタCdは、提示された原著作権ラベルL0の正当性を原著作権ラベル指紋F0によって確認して、第1加工ラベルLe1を登録するとともに、第1加工ラベルLe1の電子指紋F1を作成し、第1加工ラベルLe1に対応させた第1加工秘密鍵Kse1をデータ管理センタの第1ユーザU1の公開鍵Kb1で暗号化し、

Ckse1kb1=E（Kse1, Kb1)

暗号化第1加工秘密鍵Ckse1kb1を第1加工ラベルLe1の電子指紋Fe1とともに、第1ユーザU1に送付する。

【0112】(9) 暗号化第1加工秘密鍵Ckse1kb1及び第1加工著作権ラベルLe1の電子指紋Fe1を配布された第1ユーザU1は、暗号化第1加工秘密鍵Ckse1kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

Kse1=D（Ckse1kb1, Kv1)

復号された第1加工鍵Kse1を用いて第1加工著作物データMe1を暗号化し、

Cme1=E（Me1, Kse1)

暗号化第1加工著作物データCme1を第1加工著作権ラベルLe1及び第1加工著作権ラベルLe1の電子指紋Fe1とともに、第2ユーザU1に転送する。以後、同様な動作が繰り返される。

【0113】第3実施例において、加工データの転送時に暗号化第1加工著作物データCme1とともに転送されるのは第1加工著作権ラベルLe1及び第1加工著作権ラベルLe1の電子指紋Fe1だけであるが、他のラベル及び電子指紋も同時に転送されるように構成することもできる。図7に示されたような複数の著作物データを利用して行う加工は著作物データの数が多い分動作が煩雑であろが、単一データを利用した加工の場合と同様にして行われるが、説明が冗長にならないように省略する。

【0114】以上説明した第1実施例，第2実施例及び第3実施例のシステムでは、著作物データは秘密鍵を用いて暗号化されており、その復号用秘密鍵及び保存・複写・転送に用いる再暗号化用秘密鍵はユーザが提示したユーザラベルに基づいてデータ管理センタにより配布される。

【0115】これらの復号用秘密鍵及び再暗号化用秘密鍵はいづれも予めデータ管理センタが正当性を認証したユーザ公開鍵によって暗号化されているから、間接的にデータ管理センタの認証を受けていることになる。また、これらの秘密鍵は転送される著作物データを暗号化するために用いられるから、最終的には転送される著作

物データに対するデータ管理センタの認証も行われていることになる。このデータ管理センタによる認証は絶対的なものであるから、PEMに代表される階層型認証システムである。

【0116】その反面、著作物データそのものはデータ管理センタに転送されることなくユーザ間を転送されるから、その過程で行われる認証はPGPに代表される水平分散型認証システムであるともいうことができる。このように、この実施例のシステムによって階層型認証システムの信頼性が高いという特長と、水平分散型認証システムの扱いが簡便であるという特長を兼ね備えた認証システムが実現される。

【0117】また、著作物データを利用するユーザの行為及び行為の内容は全てユーザが提示したユーザラベルによりデータ管理センタに把握される。そして、著作物の加工を含む利用は全てデータ管理センタを経由して行われるから、各ユーザの本人確認が確実に行われるとともに、行為の内容及び経過を確認することにより、著作物データの内容及び履歴の証明が行われる。この内容証明を電子商取引等に適用した場合には、データ管理センタによる取引内容の証明、すなわち「電子公証」をすることが可能である。また、ユーザラベルにあるいは加工ラベルにデジタル署名がされている場合、ユーザラベルにあるいは加工ラベルにコンピュータウィルスが侵入すると、ラベルのデータが変化し、その結果ハッシュ値が変化する。したがって、デジタル署名を検証することによってコンピュータウィルスの侵入を検出することができる。デジタル署名を行わなくてもハッシュ値化が行われれば、変化したハッシュ値によってはユーザラベルにあるいは加工ラベルが無効であるから、コンピュータウィルスの侵入を検出することができる。

【0118】［第4実施例］ライセンスネットワークシステムに代表される分散オブジェクトシステムの場合には、大容量のデータ保存装置を有する従来のコンピュータではなく、データ保存装置を有せずデータの入出力及びデータの処理のみを行うネットワークコンピュータの使用が考慮されている。さらには、データ処理装置すら有せずデータの入出力機能のみを有する、大型コンピュータのターミナル装置的なネットワークコンピュータを使用することも考慮されている。このようなネットワークコンピュータはデータ保存装置を有していないため著作物データを保存あるいは複写することはできない。

【0119】次に、このような分散オブジェクトシステムで使用されるデータ保存装置を有していないネットワークコンピュータに対しても適用可能な実施例を説明するが、この実施例は通常のデータ保存装置を有するコンピュータに対しても適用可能であることは当然のことである。

【0120】データ著作権を保護するには著作物の無許可利用を制限するために、何らかの暗号技術を使用する必要がある。これまで説明した第1実施例、第2実施例及び第3実施例では通常のデータ保存装置を有するコンピュータを対象としたシステムでの著作権を保護するために、暗号化された著作物データと、著作物データを利用するための手がかりとして暗号化されていないラベルを用いている。これに対して、ターミナル装置的な機能しか有していないネットワークコンピュータを対象としたシステムにおいては、著作物データが保存、複写あるいは転送されることはないため著作物データを暗号化する必要はない。

【0121】第3実施例で説明したように、データ著作物の加工は、原著作物データを加工ツールを用いて改変することによって行われ、加工によって得られた加工著作物データは、利用した原著作物データ、使用した加工ツールの情報及び加工シナリオによって表現することができる。このことは分散オブジェクトシステムについても同様であり、分散オブジェクトシステム上に存在するデータベースの著作物データを利用して加工著作物データを作成した場合にも、利用したデータベース、利用した原著作物データ、使用した加工ツールの情報及び加工シナリオを特定することによって加工著作物データを再現することができ、このことは単一のデータベースあるいは複数のデータベースから入手した複数の著作物データを利用した場合であっても同様である。

【0122】図11により第4実施例を説明する。この実施例において、著作物データを保有している原著作権者及び情報提供業者（IP）は著作物データを保有していないユーザと区別されてデータ管理センタ等とともにネットワーク側に配置される。この実施例のシステムにおいては公開鍵及び専用鍵が使用される。なお、原著作物データがユーザに転送されるときには、安全のために原著作物データは秘密鍵をあるいは転送先の公開鍵を用いて暗号化される。

【0123】第1ユーザU1はネットワーク、放送あるいは記録媒体を利用して、著作物データの探索を行い必要な著作物データを収集するが、収集された著作物データはユーザU1のメモリ上に1次的に保存されるに止まり、ハードディスクドライブ（HDD）等のデータ保存装置がユーザU1の装置に含まれている場合でも著作物データがデータ保存装置に保存されることはない。著作物データが保存されることがないようにするために、保存が行われようとした場合に、メモリ上の著作物データの破壊、メモリ上のデータヘッダの変更、データの一方向ハッシュ値化、ファイル名の保存不能ファイル名への変更等が行われることにより著作物データの保存禁止が行われる。保存禁止は、オブジェクト構造を有する著作物データのプログラム部分に内蔵されたデータ保存禁止プログラムによって行うこともできるが、システム全体あるいはユーザの装置に関わるオペレーティングシステム（OS）によって行われることにより高度の信頼性が

得られる。

【0124】第4実施例は、複数の著作物データを利用する場合について説明する。(1),(2) 第1ユーザU1は第1ユーザラベルLu1を、データ管理センタに提示して、システム内の情報提供者IPのデータライブラリから原著作物データM0i (i=1,2,3...)を収集し、加工ツールPeを入手するが、このとき原著作物データM0i及び加工ツールPeは第1ユーザU1の公開鍵Kb1を用いて暗号化されて、

Cm0ikb1=E (M0i, Kb1)

Cpekb1=E (Pe, Kb1)

暗号化原著作物データCm0ikb1及び暗号化加工ツールCpekb1が、第1ユーザU1に配付される。なお、このとき第1ユーザラベルLu1が参照されることにより、原著作物データM0i及び加工ツールPeの利用状況もデータ管理センタに記録され、課金に利用される。

【0125】(3) 暗号化原著作物データCm0ikb1及び暗号化加工ツールCpekb1を配布された第1ユーザU1は、配布された暗号化原著作物データCm0ikb1及び暗号化加工ツールCpekb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

M0i=D (Cm0ikb1, Kv1)

Pe=D (Cpekb1, Kv1)

し、復号された加工ツールPeを使用して復号された原著作物データM0iを加工し、第1加工著作物データM1i (i=1,2,3...)を得る。

【0126】(4) 第1加工著作物データM1iを得た第1ユーザU1は、第1加工著作物データM1iについての加工データである第1シナリオS1iをデータ管理センタの公開鍵Kbcで暗号化し、

Cs1ikbc=E (S1i, Kbc)

暗号化第1シナリオCs1ikbcを第1ユーザラベルLu1とともに、データ管理センタCdに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【0127】(5) 暗号化第1シナリオCs1ikbcを提示されたデータ管理センタCdは、暗号化第1シナリオCs1ikbcをデータ管理センタCdの専用鍵Kvcを用いて復号し、

S1i=D (Cs1ikbc, Kvc)

提示された第1ユーザU1のユーザラベルと復号された第1加工シナリオS1iに基づき第1加工ラベルLe1を作成し、データ管理センタCd内に保管し、第1加工ラベルLe1を第1ユーザU1の公開鍵Kb1を用いて暗号化し、

C1e1kb1=E (Le1, Kb1)

暗号化第1加工ラベルC1e1kb1を、第1ユーザU1に転送する。

【0128】(6) 暗号化第1加工ラベルC1e1kb1を転送された第1ユーザU1は、暗号化第1加工ラベルC1e1kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

Le1=D (C1e1kb1, Kv1)

復号された第1加工ラベルLe1を第2ユーザU2の公開鍵Kb2を用いて暗号化し、

C1e1kb2=E (Le1, Kb2)

暗号化第1加工ラベルC1e1kb2を、第2ユーザU2に転送するが、第1加工著作物データM1iあるいは暗号化第1加工著作物データが第2ユーザU2に転送されることはない。

【0129】第1ユーザU1のコンピュータがデータ保存装置を有しているときには収集著作物データあるいは加工データがデータ保存装置に保存される可能性があるが、保存・複写及び転送を阻止するために、上述の保存禁止が行われる。なお、この場合暗号化第1加工ラベルC1e1kb2の代わりに、第1加工ラベルを一方向ハッシュ値化した電子指紋F1を使用することもでき、このようにすることにより電話音声による簡略化された加工ラベルの転送が可能になる。

【0130】(7) 暗号化第1加工ラベルC1e1kb2を転送された第2ユーザU2は、転送された暗号化第1加工ラベルC1e1kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

Le1=D (C1e1kb2, Kv2)

第1加工ラベルLe1を第2ユーザU2の専用鍵Kv2を用いて暗号化し、

C1e1kv2=E (Le1, Kv2)

暗号化第1加工ラベルC1e1kv2を第2ユーザラベルLu2とともに、データ管理センタCdに提示する。

【0131】(8) 暗号化第1加工ラベルC1e1kv2と第2ユーザラベルLu2を提示されたデータ管理センタCdは、提示された暗号化第1加工ラベルC1e1kv2を第2ユーザU2の公開鍵Kb2を用いて復号し、

Le1=D (C1e1kv2, Kb2)

復号された第1加工ラベルLe1に記載された原著作物データM0iを収集し、原著作物データM0iを加工ツールPeを用いて同じく第1加工ラベルLe1に記載された第1シナリオS1iに基づいて加工して第1加工著作物データM1iを再生する。

【0132】第1加工著作物データM1iを再生したデータ管理センタCdは、第1加工著作物データM1i及び加工ツールPeを第2ユーザU2の公開鍵Kb2を用いて暗号化し、

Cm1ikb2=E (M1i, Kb2)

Cpekb2=E (Pe, Kb2)

暗号化第1加工著作物データCm1ikb2及び暗号化加工ツールCpekb2を、第2ユーザU2に転送する。

【0133】(9) 暗号化第1加工著作物データCm1ikb2及び暗号化加工ツールCpekb2を配布された第2ユーザU2は、配布された暗号化第1著作物データCm1ikb2及び暗号化加工ツールCpekb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

M1i＝D（Cm1ikb2，Kv2）
Pe＝D（Cpekb2，Kv2）
し、復号された加工ツールPeを使用して復号された第1加工著作物データM1iを加工し、第2加工著作物データM2i(i=1,2,3...)を得る。

【0134】(10) 第2加工著作物データM2iを得た第2ユーザU2は、第2加工著作物データM2iについての加工データである第2シナリオS2iをデータ管理センタの公開鍵Kbcで暗号化し、
Cs2ikbc＝E（S2i，Kbc）
暗号化第2シナリオCs2ikbcを第2ユーザラベルLu2とともに、データ管理センタCdに提示する。

【0135】(11) 暗号化第2シナリオCs2ikbcを提示されたデータ管理センタCdは、暗号化第2シナリオCs2ikbcをデータ管理センタCdの専用鍵Kvcを用いて復号し、
S2i＝D（Cs2ikbc，Kvc）
提示された第2ユーザU2のユーザラベルと復号された第2加工シナリオS2iに基づき第2加工ラベルLe2を作成し、データ管理センタCd内に保管し、第2加工ラベルLe2を第1ユーザU2の公開鍵Kb2を用いて暗号化し、
C1e2kb2＝E（Lei，Kb2）
暗号化第2加工ラベルC1e2kb2を、第2ユーザU2に転送する。

【0136】(12) 暗号化第2加工ラベルC1e2kb2を転送された第2ユーザU2は、暗号化第2加工ラベルC1e2kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、
Le2＝D（C1e2kb2，Kv2）
復号された第2加工ラベルLe2を第3ユーザU3の公開鍵Kb3を用いて暗号化し、
C1e2kb3＝E（Le2，Kb3）
暗号化第2加工ラベルC1e2kb3を、第3ユーザU3に転送する。以後、同様な動作が繰り返される。

【0137】この分散オブジェクトシステムを利用する第4実施例では、著作物データはユーザが保存せず、データベースにのみ保存されている、一方ユーザはユーザの情報に加工に関する情報すなわち、利用した原著作物データ，使用した加工ツールの情報及び加工シナリオ及び加工したユーザ情報が記載された加工ラベルのみを管理保存し、この加工ラベルのみが暗号化されてユーザ間で転送される。したがって、著作物データが保存・複写あるいは転送されることはない。

【0138】また、この実施例のシステムにおいては公開鍵及び専用鍵のみが使用され、この公開鍵は予めデータ管理センタによって正当性が認証されており、このデータ管理センタによる認証は絶対的なものであるから、PEMに代表される階層型認証システムである。そして、転送される加工ラベルは予めデータ管理センタが正当性を認証したユーザ公開鍵によって暗号化されて転送されるから、その内容は間接的にデータ管理センタの認証を受けた確実性があるものであることになる。この、加工ラベルそのものはデータ管理センタに転送されることなくユーザ間を転送されるから、その過程で行われる認証はPGPに代表される水平分散型認証システムであるともいうことができる。このように、この実施例のシステムによって階層型認証システムの信頼性が高いという特長と、水平分散型認証システムの扱いが簡便であるという特長を兼ね備えた認証システムが実現される。

【0139】また、著作物データを利用するユーザの行為及び行為の内容は全てユーザが提示したユーザラベルによりデータ管理センタに把握される。そして、著作物の加工を含む利用は全てデータ管理センタを経由して行われるから、各ユーザの本人確認が確実に行われるとともに、行為の内容及び経過を確認することにより、著作物データの内容及び履歴の証明が行われる。この内容証明を電子商取引等に適用した場合には、データ管理センタによる取引内容の証明、すなわち「電子公証」をすることが可能である。

【0140】さらに、ユーザラベルにあるいは加工ラベルにデジタル署名がされている場合、ユーザラベルにあるいは加工ラベルにコンピュータウィルスが侵入すると、ラベルのデータが変化し、その結果ハッシュ値が変化する。したがって、デジタル署名を検証することによってコンピュータウィルスの侵入を検出することができる。デジタル署名を行わなくてもハッシュ値化が行われれば、変化したハッシュチによってはユーザラベルにあるいは加工ラベルが無効であるから、コンピュータウィルスの侵入を検出することができる。

【0141】また、この実施例でも、著作物データを利用するユーザの行為及び行為の内容は全てユーザが提示したユーザラベルによりデータ管理センタに把握されているため、上記の課金方式の何れもが有効に機能する。

【0142】［第5実施例］本発明のシステムを電子商取引に適用する実施例を説明するが、初めに、すべての処理が仲介業者を通じて行われる基本的な場合について図12（a）により説明する。

(1) ユーザ（需要者）Uは、ネットワークを介して仲介業者Sの商品カタログを閲覧し、購入を希望する商品の発注に関する見積書，発注書フォーム及び決済情報等の取引データQmを仲介業者Sに要求する。

【0143】(2) 取引データQmの要求を受けた仲介業者Sは、ユーザUからなされた取引データQmの要求R及び第1秘密鍵Ks1をメーカ（生産者）Mの公開鍵Kbmを用いて暗号化し、
Crkbm＝E（R，Kbm）
Cks1kbm＝E（Ks1，Kbm）
暗号化要求Crkbm及び暗号化第1秘密鍵Cks1kbmをメーカMに送付する。

【0144】(3) 暗号化要求Crkbm及び暗号化第1秘密

35

鍵Cks1kbmを送付されたメーカMは、送付された暗号化要求Crkbm及び暗号化第1秘密鍵Cks1kbmをメーカMの専用鍵Kvmを用いて復号し、

R＝D（Crkbm，Kbm）

Ks1＝D（Cks1kbm，Kbm）

要求Rに対応する取引データQmを復号された第1秘密鍵Ks1を用いて暗号化して、

Cqmks1＝E（Qm，Ks1）

暗号化取引データCqmks1を仲介業者Sに送付する。

【0145】(4) 暗号化取引データCqmks1を送付された仲介業者Sは、送付された暗号化取引データCqmks1を第1秘密鍵Ks1を用いて復号し、

Q＝D（Cqks1，Ks1）

復号された取引データQmを第2秘密鍵Ks2を用いて再度暗号化し、

Cqmks2＝E（Qm，Ks2）

第2秘密鍵KS2をユーザの公開鍵Kbuを用いて暗号化し、

Cks2kbu＝E（Ks2，Kbu）

暗号化取引データCqmks2及び暗号化第2秘密鍵Cks2kbuをユーザUに送付する。

【0146】(5) 暗号化取引データCqmks2及び暗号化第2秘密鍵Cks2kbuを送付されたユーザUは、暗号化第2秘密鍵Cks2kbuをユーザUの専用鍵Kvuを用いて復号し、

Ks2＝D（Cks2kbu，Kvu）

復号された第2秘密鍵Ks2を用いて暗号化取引データCqmks2を復号し、

Qm＝D（Cqmks2，Ks2）

復号された取引データQmに発注内容を記入することによりデータの加工を行って発注書Quを作成し、作成した発注書Quを第2秘密鍵Ks2を用いて暗号化し、

Cquks2＝E（Qu，Ks2）

暗号化発注書Cquks2を仲介業者Sに送付する。

【0147】(6) 暗号化発注書Cquks2を送付された仲介業者Sは、暗号化発注書Cquks2を第2秘密鍵Ks2を用いて復号し、

Qu＝D（Cquks2，Ks2）

復号された発注書QuをメーカMの公開鍵Kbmを用いて暗号化し、

Cqukbm＝E（Qu，Kbm）

暗号化発注書CqukbmをメーカMに転送する。

【0148】暗号化発注書Cqukbmを転送されたメーカMは、メーカMの専用鍵Kvmを用いて暗号化発注書Cqukbmを復号し、

Qu＝D（Cqukbm，Kvm）

復号された発注書Quの内容にしたがって、受注処理を行う。

【0149】次に、ユーザがメーカに対して直接に発注を行った場合の例外的な処理について図12（b）により説明する。なお、この例外的な場合において上述(4)の暗号化取引データCqmks2及び暗号化第2秘密鍵Cks2kbuがユーザUに送付される段階までは、図12（a）に示された基本的な場合と同様なので再度の説明は省略し、基本的な場合と異なっている段階についてのみ説明する。

36

【0150】(7) 暗号化取引データCqmks2及び暗号化第2秘密鍵Cks2kbuを送付されたユーザUは、暗号化第2秘密鍵Cks2kbuをユーザUの専用鍵Kvuを用いて復号し、

Ks2＝D（Cks2kbu，Kvu）

復号された第2秘密鍵Ks2を用いて暗号化取引データCqmks2を復号し、

Qm＝D（Cqmks2，Ks2）

復号された取引データQmに発注内容を記入することによりデータの加工を行って発注書Quを作成し、作成した発注書Quを第2秘密鍵Ks2を用いて暗号化し、

Cquks2＝E（Qu，Ks2）

暗号化発注書Cquks2をメーカMに送付する。

【0151】(8) 暗号化発注書Cquks2を送付されたメーカMは、暗号化発注書Cquks2を販売業者Sに転送する。

【0152】(9) 暗号化発注書Cquks2を転送された仲介業者Sは、第2秘密鍵Ks2を用いて暗号化発注書Cquks2を復号し、

Qu＝D（Cquks2，Ks2）

復号された発注書QuをメーカMの公開鍵Kbmを用いて暗号化し、

Cqukbm＝E（Qu，Kbm）

メーカMに転送する。

(10) 暗号化発注書Cqukbmを転送されたメーカMは、メーカMの専用鍵Kvmを用いて暗号化発注書Cqukbmを復号し、

Qu＝D（Cqukbm，Kvm）

発注書Quの内容にしたがって、受注処理を行う。

【0153】この商取引の対象になる商品は物品以外に、ネットワークを介して行われるコンピュータソフトウェアも対処とすることが可能である。その場合に取引されるソフトウェアPはメーカMがメーカの専用鍵Kvmを用いて暗号化し、

Cpkvm＝E（P，Kvm）

暗号化ソフトウェアCpkvmを仲介業者Sに転送し、転送された暗号化ソフトウェアCpkvmを仲介業者SがメーカMの公開鍵Kbmを用いて復号し、

P＝D（Cpkvm，Kbm）

仲介業者Sが復号されたソフトウェアPをユーザUの公開鍵Kbuを用いて暗号化し、

Cpkbu＝E（P，Kbu）

暗号化ソフトウェアCpkbuをユーザUに転送し、転送された暗号化ソフトウェアCpkbuをユーザUが専用鍵Kvu

37

を用いて復号する。

$P = D(C_{pkbu}, K_{vu})$

【０１５４】さらに、ＣＤ－ＲＯＭ等の蓄積媒体に保存された暗号化ソフトウェアの暗号鍵を有料で配布することが行われているが、この暗号鍵もここで述べたコンピュータソフトウェアと同様な方法により商取引の対象とすることができる。

【０１５５】図１２（ａ）で説明された基本的な場合において、取引の全てが仲介業者を通じて行われるため、取引過程から仲介業者が除外されることによる種々の障害の発生は未然に防止される。また、図１２（ｂ）で説明された例外的な場合においても、発注書の内容をメーカが知り受注処理を行うためには、暗号化発注書を仲介業者に転送し、仲介業者によって復号化してもらう必要がある。したがって、この場合にも取引過程に必ず仲介業者が関与することになるため、取引過程から仲介業者が除外されることによる種々の障害の発生は同様に未然に防止される。なお、送付される秘密鍵は単独で送付される他に取引データ中に組み込んで送付することもできる。

【図面の簡単な説明】

38

＊【図１】ラベルの説明図。

【図２】ラベル、データヘッダ、データボディの説明図。

【図３】ラベルとデータの暗号化の説明図。

【図４】データヘッダとデータボディの暗号化の説明図。

【図５】ラベル、データヘッダ及びデータボディの暗号化の説明図。

【図６】オブジェクトファイル暗号化の説明図。

【図７】本発明第１実施例のデジタルデータ管理システムの概要構成図。

【図８】本発明第２実施例のデジタルデータ管理システムの概要構成図。

【図９】複数データから１つのデータを生成する技術の説明図。

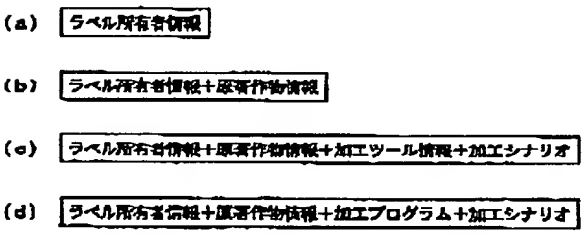
【図１０】本発明第３実施例のデジタルデータ管理システムの概要構成図。

【図１１】本発明第４実施例のデジタルデータ管理システムの概要構成図。

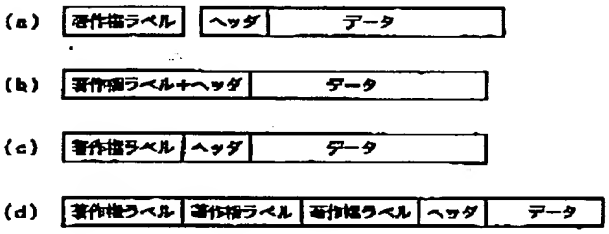
【図１２】本発明第３実施例のデジタルデータ管理システムの概要構成図。

＊

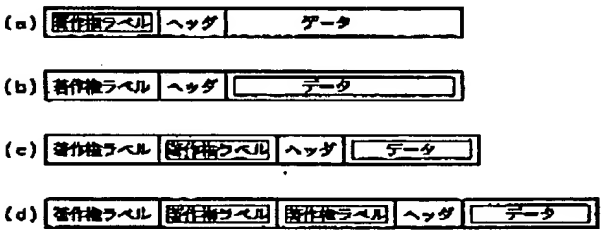
【図１】



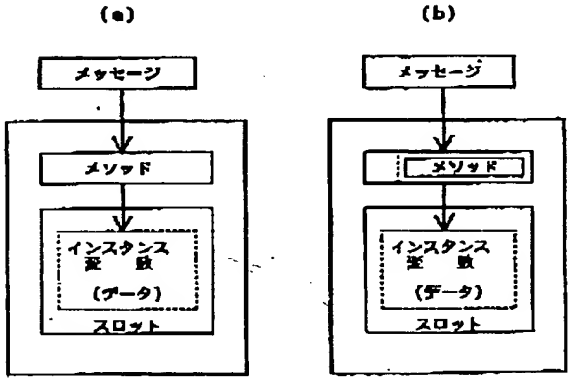
【図２】



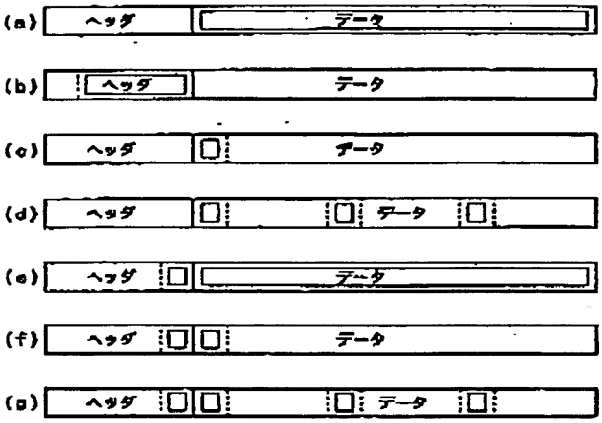
【図３】



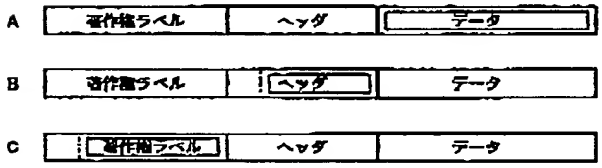
【図６】



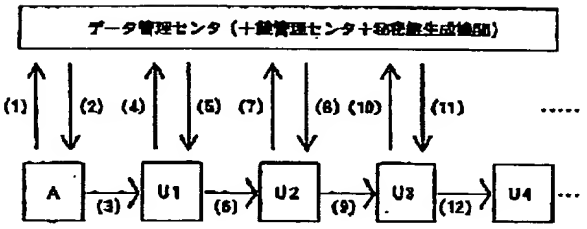
【図4】



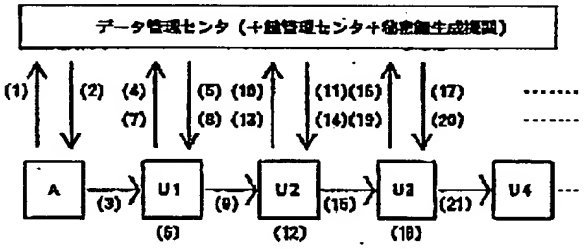
【図5】



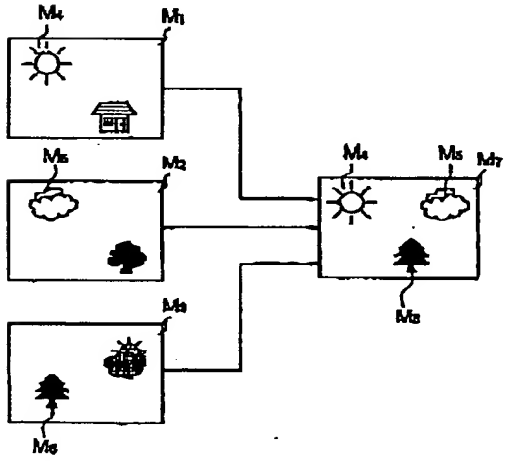
【図7】



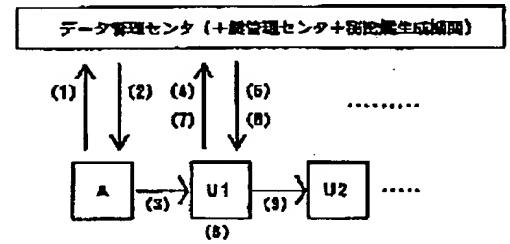
【図8】



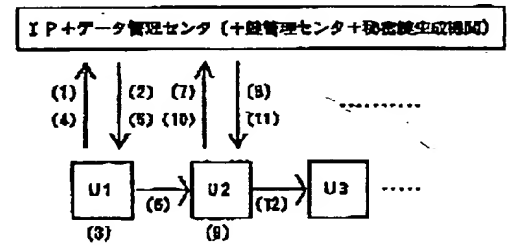
【図9】



【図10】

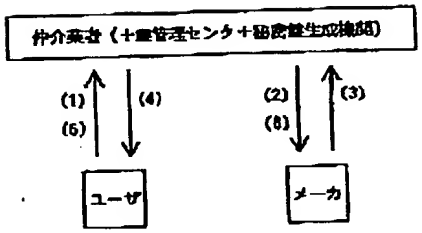


【図11】

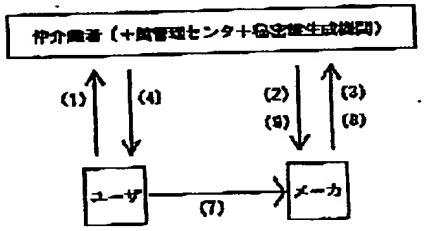


【図12】

(a)



(b)



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/32		H04L 9/00	675D